

Jeffrey D. Vanacore
JVanacore@perkinscoie.com
Todd M. Hinnen (admitted *pro hac vice*)
THinnen@perkinscoie.com
PERKINS COIE LLP
30 Rockefeller Plaza, 22nd Floor
New York, NY 10112-0085
Telephone: 212.262.6900
Facsimile: 212.977.1649
Attorneys for Nonparty Google Inc.

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

**In re Search Warrant Mag. No.
16-4116 (MAH) to Google Inc.**

Mag. No. 16-4116

Hon. Michael A. Hammer

GOOGLE INC.'S OBJECTIONS TO MAGISTRATE ORDER
AND MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT

TABLE OF CONTENTS

	Page
OBJECTIONS.....	1
MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT	3
I. INTRODUCTION	3
II. FACTUAL BACKGROUND.....	7
III. ARGUMENT.....	7
A. The SCA’s warrant provision does not authorize searches of data stored extraterritorially	10
B. Requiring a provider to execute a warrant to search and seize data outside the United States is an impermissible extraterritorial application of the SCA	15
1. The SCA’s focus is protection of the privacy of electronic communications by regulating the particular means of compelling disclosure.....	16
2. Assisting in the execution of an SCA warrant is conduct that is necessary to the operation of the statute and therefore relevant to its focus.....	18
C. The Court should decline to weigh policy interests Congress has not yet considered	23
IV. CONCLUSION.....	26

TABLE OF AUTHORITIES

CASES	Page(s)
<i>Benz v. Compania Naviera Hidalgo, S.A.</i> , 353 U.S. 138 (1957).....	25
<i>Connecticut Nat’l Bank v. Germain</i> , 503 U.S. 249 (1992).....	13
<i>F.A.A. v. Cooper</i> , 132 S. Ct. 1441 (2012).....	12
<i>In re 381 Warrants Direct to Facebook, Inc.</i> , ___ N.E.3d ___, 2017 WL 1216079, 2017 N.Y. Slip Op. 02586 (N.Y. Apr. 4, 2017)	13
<i>In re Search of Content that Is Stored At Premises Controlled by Google</i> , No. 16-mc-80263, 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017).....	8
<i>In re Search of Info. Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc.</i> , No. 16-mj-757 (GMH), 2017 WL 2480752 (D.D.C. June 2, 2017).....	8
<i>In re Search Warrants to Google</i> , Nos. 16-960-M-01, 16-1061-M, ___ F. Supp. 3d ___, 2017 WL 471564 (E.D. Pa. Feb. 3, 2017)	8, 11
<i>In re Two email accounts stored at Google Inc.</i> , No. 17-M-1235, 2017 WL 2838156 (E.D. Wis. June 30, 2017)	8
<i>In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.</i> , 829 F.3d 197 (2d Cir. 2016), <i>reh’g denied en banc</i> , 855 F.3d 53 (2d Cir. Jan. 24, 2017)	<i>passim</i>
<i>Molzof v. United States</i> , 502 U.S. 301, 307 (1992).....	<i>passim</i>

<i>Morrison v. Nat’l Australia Bank Ltd.</i> , 561 U.S. 247 (2010).....	<i>passim</i>
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014).....	20
<i>RJR Nabisco, Inc. v. European Cmty.</i> , 136 S. Ct. 2090 (2016).....	<i>passim</i>
<i>United States v. Bach</i> , 310 F.3d 1063 (8th Cir. 2002)	13
<i>United States v. Jefferson</i> , 571 F. Supp. 2d 696 (E.D. Va. 2008)	22
<i>United States v. Verdugo-Urquidez</i> , 494 U.S. 259 (1990).....	13
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010)	19
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978).....	14

STATUTES

Stored Communications Act (18 U.S.C. § 2701 <i>et. seq.</i>).....	<i>passim</i>
18 U.S.C. § 2518(3)	12
28 U.S.C. § 636(b)(1)(B),(C).....	1

RULES

Civ. L. R. 72.1	1
Fed. R. Civ. P. 72(a).....	1
Fed. R. Crim. P. 41.....	12, 14
Fed. R. Crim. P. 59(a)	1

OTHER AUTHORITIES

132 Cong. Rec. S7991 (daily ed. June 19, 1986) (statement of Sen. Leahy)	16-17
Council Regulation (EC) No 2271/96 of 22 November 1996 (E.U. Blocking Statute)	22
Federal Data Protection Act of 14 August 2009 (Federal Law Gazette I p. 2814) (German Blocking Statute)	23
H.R. Rep. No. 99-647 (1986).....	13
International Communications Privacy Act, S. 2986, H.R. 5323, 114th Cong. (2016) available at https://www.aclu.org/sites/default/files/ field_document/doj_legislative_proposal.pdf	24
Law no. 80-538 of 16 July 1980 (French Blocking Statute).....	23
Letter from Mythili Raman, Acting Assistant Attorney General, to Judge Reena Raggi, Chair Advisory Comm. on the Criminal Rules (Sep. 18, 2013) (available at https://www.justsecurity.org/wp- content/uploads/2014/09/Raman-letter-to-committee-.pdf)	14
Letter from Peter J. Kadzik, Assistant Attorney General, Dep't of Justice Office of Legislative Affairs, to Hon. Joseph A. Biden, President of the Senate, at p. 1 (July 15, 2016), https://www.aclu.org/sites/default/files/field_document/doj_legisla tive_proposal.pdf (last visited July 21, 2017).....	24
Orin Kerr, <i>A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it</i> , 72 Geo. Wash. L. Rev. 1208, 1218 (2004).....	18
Orin Kerr, <i>Fourth Amendment Seizures of Computer Data</i> , 119 Yale L.J. 700, 703 (2010)	22
Orin Kerr, <i>The Next Generation Communications Privacy Act</i> , 162 U. Pa. L. Rev. 373, 384 (2014).....	19, 25
S. Rep. No. 99-541 (1986), <i>reprinted in</i> 1986 U.S.C.C.A.N. 3555	16

U.S. Department of Justice, <i>Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations</i> (2009) , https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf (last visited June 30, 2017)	17, 22, 23
Yvonne Lee, <i>Compuserve, MCI Mail Introduce Gateways to Internet Network</i> , InfoWorld, Sept. 25, 1989	6

OBJECTIONS

Pursuant to 28 U.S.C. § 636(b)(1)(B),(C), Fed. R. Civ. P. 72(a), Fed. R. Crim. P. 59(a), and Civ. L. R. 72.1, Google objects to the Memorandum Opinion granting the government's motion to compel compliance with a search warrant. *See In re Search Warrant to Google, Inc.*, Mag. No. 16-4116, (D.N.J. July 10, 2017) (hereinafter, "Decision"). Google objects for the following reasons as further discussed in Google's Memorandum in Support:

1. The Magistrate Judge erred in concluding "that compelling Google to provide all responsive information to the search warrant issued in this matter, regardless of whether the information is stored on computer servers outside of the United States, does not violate the presumption against extraterritorial application of United States law." Decision at 20. This conclusion is contrary to *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), which held that searching and seizing data outside the United States so that it could be produced in response to a warrant issued pursuant to the Stored Communications Act, 18 U.S.C. § 2701 *et seq.* ("SCA"), did constitute an unlawful extraterritorial application of the SCA.

2. The Magistrate Judge erred in finding that the "conduct relevant to the extraterritorial analysis — *i.e.*, the location of the search — occurs entirely in the United States." Decision at 20. In *Morrison v. Nat'l Australia Bank Ltd.*, the

Supreme Court set forth a two-part test to determine whether a statute has extraterritorial reach. 561 U.S. 247, 261-62 (2010). That test requires a court to consider whether “conduct relevant to the statute’s focus” occurs outside the United States. *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2101 (2016) (interpreting *Morrison*). In situations where the communications sought by a warrant are located outside the United States, assistance in the execution of a warrant requires Google to engage in essential conduct outside the United States, including writing queries that permit searches of datacenters in different locations; executing those queries to search Google’s network to identify responsive data; and retrieving responsive data from wherever on Google’s network that data resides. In cases such as this one, conduct necessary to assist in execution of the warrant would take place outside of the United States. Thus, requiring Google to produce foreign-stored data in response to the warrant would be an impermissible extraterritorial application of the SCA.

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT

I. INTRODUCTION

This matter involves a search warrant issued under the Stored Communications Act (“SCA”), that purports to require Google Inc. (“Google”) to search for customer communications stored in locations both inside and outside the United States, and seize them for the government. *In re Search Warrant to Google, Inc.*, Mag. No. 16-4116, (D.N.J. July 10, 2017) (hereinafter, “Decision”). Google has, to the best of its current capabilities, searched its data centers in the United States, seized the customer communications within the scope of the warrant, and produced those communications to the government. The question raised by this matter is whether the warrant lawfully requires Google to identify, access, and retrieve customer communications stored in data centers located outside the United States and to disclose those communications to the government despite the fact that the warrant does not and could not authorize the government to access foreign data centers to obtain the same information without Google’s assistance.

The U.S. Court of Appeals for the Second Circuit — the only Circuit Court to have addressed the issue — properly held that an SCA warrant cannot compel a service provider to search data centers and seize customer communications located outside the United States. *In re Warrant to Search a Certain E-Mail Account*

Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016) (“*Second Circuit Decision*”). When Congress enacted the SCA, it did not consider the complex policy issues raised by warrants that seek foreign-stored data. Accordingly, Congress did not authorize the use of warrants to reach communications held solely on servers abroad. Furthermore, in accordance with the presumption against extraterritoriality — a well-established canon of statutory interpretation set out in *Morrison v. Nat’l Australia Bank Ltd.*, 561 U.S. 247 (2010) — a statute does not apply to conduct outside the United States absent a clear indication that Congress intended it to do so.

Despite the Supreme Court’s repeated emphasis in recent years on the importance of the presumption against extraterritoriality, the Magistrate Judge’s Decision fails to apply that presumption properly. The Magistrate Judge held that a provider’s disclosure of customer communications stored outside the United States does not implicate extraterritorial concerns, in part because the “warrant calls for a search and not a seizure, and that the conduct relevant to the extraterritorial analysis — *i.e.*, the location of the search — occurs entirely in the United States.” Decision at 20. The Magistrate Judge thus held that Google’s conduct in accessing foreign data centers to identify responsive communications, and then retrieving those communications to the United States for disclosure to the government was not conduct relevant to the focus of the SCA and thus would “not

violate the presumption against extraterritorial application of United States law.”

Id.

Respectfully, the Decision is incorrect. By confining the analysis to the narrow question of whether, in executing an SCA warrant, a constitutional search or seizure occurs entirely in the United States, *see* Decision at 20-24, the Decision fails to take into account both the focus of the SCA and conduct essential to that focus. The SCA is focused on protecting the privacy of electronic communications entrusted to service providers by regulating the conditions under which access to and disclosure of those communications may or may not occur. Section 2703 supports the SCA’s privacy focus by requiring the government to obtain a search warrant (as opposed to a subpoena or order) in order to compel a provider to assist in the execution of a search and seizure of communications content. But regardless of whether the statute’s focus is privacy, or as the government has suggested, disclosure, *see* Decision at 20 n.6, the result is the same. By requiring Google to locate, access, and retrieve communications stored outside the United States, the warrant requires Google to engage in conduct outside of the United States that is not only relevant to the SCA’s focus, but essential to the effectiveness of Section 2703.

Interpretation of the SCA’s warrant provision no doubt implicates many policy questions. Thirty-one years ago, when Congress enacted the SCA, the

Internet was in its infancy. Public access to the Internet would not be available for another three years. *See* Yvonne Lee, *Compuserve, MCI Mail Introduce Gateways to Internet Network*, InfoWorld, Sept. 25, 1989 at 32 (reporting availability of first public gateways to the Internet). Congress did not foresee the more-than-3-billion-user global network supporting myriad communication, personal, and commercial services that the Internet has become, nor did it consider the complex policy and diplomatic issues raised by government requests for communications stored on such a worldwide network.

Congress should consider these difficult policy issues, hear from all stakeholders in an open, public debate, and reform and modernize the statute. A court, confined as it is to the single case or controversy before it, has neither the institutional competence nor the constitutional authority to amend the law. The Court should leave to Congress the legislative responsibility of amending the SCA, give effect to its plain language, and hold that a warrant issued pursuant to its terms cannot require a service provider to identify, access, and retrieve to the United States customer communications stored in foreign data centers. For these reasons, the Court should amend the warrant to require Google to produce only those communications stored in the United States.

II. FACTUAL BACKGROUND

On December 19, 2016, the government obtained a search warrant purporting to compel Google to search for, seize, and disclose customer records, including customer communications, relating to a number of Google accounts. *See* Decision at 1; Stipulation of Facts (“Stip.”) at ¶ 6 (attached as Ex. A). In response, Google produced responsive materials that it confirmed at the time were stored in the United States. *See* Decision at 2; Stip. at ¶ 7. Consistent with the SCA and the *Second Circuit Decision*, Google did not produce data stored outside the United States. *See* Decision at 2. On April 21, 2017, the government moved to compel Google to produce information sought by the warrant that is stored entirely outside of the United States, and Google opposed the government’s motion. *Id.* at 2-3. Magistrate Judge Hammer issued the Decision on July 10, 2017. Google now timely files its objections and this memorandum in support thereof.

III. ARGUMENT

A unanimous panel of the U.S. Court of Appeals for the Second Circuit Court has held that an SCA warrant can compel a provider to produce only customer records stored in the United States. *Second Circuit Decision*, 829 F.3d at 222. An SCA warrant cannot compel a provider to produce records stored outside the United States. *Id.* The Second Circuit recently denied the government’s petition for rehearing *en banc* (although four judges dissented from the denial). *En*

Banc Denial, 855 F.3d 53 (2d Cir. 2017). No other Court of Appeals has addressed the issue.¹

In this case, the Magistrate Judge correctly held that the SCA does not apply extraterritorially. *See* Decision at 19. In so holding, the Magistrate Judge rejected the government's argument that an SCA warrant is an *in personam* exercise of the court's jurisdiction, instead noting that SCA warrants, like ordinary warrants, are subject to territorial limitations and cannot be executed abroad. *See id.* at 16-17. The Magistrate Judge further rejected the government's argument that a subsequent international convention had any bearing on the intent of Congress at

¹ Several magistrate judges have entered unsealed opinions departing from the Second Circuit *Decision* in cases involving Google. *In re Two email accounts stored at Google, Inc.*, No. 17-M-1235, 2017 WL 2838156, at *3 (E.D. Wis. June 30, 2017) (“*EDWI Order*”); *In re Search of Info. Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757 (GMH), 2017 WL 2480752, at *11 (D.D.C. June 2, 2017) (“*DDC Order*”); *In re Search of Content that Is Stored At Premises Controlled by Google*, No. 16-mc-80263-LB, 2017 WL 1487625, at *4 (N.D. Cal. Apr. 25, 2017) (“*NDCA Order*”); *In re Search Warrants to Google*, Nos. 16-960-M-01, 16-1061-M, __ F. Supp. 3d ___, 2017 WL 471564, at *11 (E.D. Pa. Feb. 3, 2017) (“*EDPA Order*”). Google has filed objections to the *EDPA*, *NDCA* and *EDWI Orders*. *See* Google Inc.’s Objections to Magistrate Order and Memorandum in Support, *In re: Two email accounts stored at Google Inc.*, No. 17-M-1235 (E.D. Wis. July 14, 2017), ECF No. 16; Google, Inc.’s Objections to Magistrate Order and Memorandum in Support, *In the Matter of Content that is Stored at Premises Controlled by Google*, No-16-mc-80263 (N.D. Cal. May 3, 2017), ECF No. 47; Google, Inc.’s Objections Magistrate’s Orders Granting Government’s Motions to Compel and Overruling Google’s Overbreadth Objection, *In re Search Warrants to Google*, No. 16-MJ-960, 16-MJ-1061 (E.D. Pa. Feb. 15, 2017), ECF No. 34. The docket for the *DDC Order*, including any subsequent filings or objections, remains under seal.

the time it enacted the SCA. *See id.* at 18-19. However, the Magistrate Judge erred when he held that Google’s identification, access, retrieval, and disclosure to the government of communications stored outside of the United States would not violate the presumption against extraterritoriality. *See id.* at 24 (finding that compelling Google to retrieve communications, “even if that data is copied from foreign servers, does not run afoul of the presumption against extraterritorial application of United States law”). In so doing, the Magistrate Judge misapplied the test established in *Morrison*. Rather than identifying the conduct relevant to the SCA’s focus and examining whether any of that relevant conduct occurs abroad, the Magistrate Judge instead examined whether a Fourth Amendment search or seizure takes place, and determined that “the location of the search [] occurs entirely in the United States.” *Id.* at 20. Contrary to the Magistrate Judge’s analysis, *Morrison* does not instruct a court to determine the locus of the relevant conduct by reference to technical constitutional concepts such as a Fourth Amendment search or seizure, or to myopically zero in on the location of a single act. It instead requires a court to identify all of the conduct that is relevant to the statute’s focus, and to examine whether any of that relevant conduct occurs outside of the United States. *See RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2101 (2010). When the effectiveness of a Section 2703 warrant depends upon steps taken by a provider to identify communications stored abroad, access foreign

servers, and to and retrieve those communications from foreign servers before disclosing them to the government, these extraterritorial actions are not only relevant to the SCA; they are necessary to its operation.

A. The SCA’s warrant provision does not authorize searches of data stored extraterritorially.

“[L]egislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.” *Morrison*, 561 U.S. at 255 (citation omitted). In *Morrison*, the Supreme Court set forth a two-part test to determine if a statute has an impermissible extraterritorial application. The first step considers “whether the statute gives a clear, affirmative indication that it applies extraterritorially.” *RJR Nabisco*, 136 S. Ct. at 2101 (describing the first step of the *Morrison* test). If the statute does not so indicate, a Court must proceed to the second step, which involves determining whether any of the “conduct relevant to the statute’s focus” — *i.e.*, any of the conduct the statute governs or is concerned with — occurs outside the United States. *Id.*; *see also Morrison*, 561 U.S. at 266-67 (identifying relevant conduct as “the objects of the statute’s solicitude” and those acts that “the statute seeks to ‘regulate’”).

As the Magistrate Judge correctly found, there should be no dispute that the SCA’s warrant provision has no application outside the United States. *See* Decision at 19 (“The Court concludes that a plain reading of the SCA reveals it does not contain a clear expression of Congressional intent of extraterritorial

application.”); *see also* *EDPA Order*, 2017 WL 471564 at *7 (E.D. Pa. Feb. 3, 2017). As the Second Circuit observed, “a globally-connected Internet available to the general public for routine e-mail and other uses was still years in the future” when Congress passed the SCA. *Second Circuit Decision*, 829 F.3d at 206. Congress therefore had no occasion to extend the warrant provision outside the United States at the time it passed the SCA, and nothing in the SCA’s text or legislative history indicates that it intended to do so.

In Section 2703 of the SCA, Congress distinguished between a “warrant,” which it generally required the government to obtain before compelling a provider to assist in searching for and disclosing customers’ private communications, and a “subpoena” or an “order,” which it required the government to obtain before compelling a provider to disclose the provider’s own business records. *Compare* 18 U.S.C. § 2703(a) *with* § 2703(c). As the Magistrate Judge implicitly acknowledged, *see* Decision at 16-17, the distinction was designed to do more than require the government to make a probable cause showing to obtain user communications; the Wiretap Act, amended by the legislation that created the SCA, had addressed a similar concern regarding the interception of customers’ communications by setting forth a procedure by which the government can apply for, and a court can grant, *an order issued on a finding of probable cause* requiring

a provider to intercept communications. *See* 18 U.S.C. § 2518(3).² If Congress had intended in Section 2703(a) to create a “probable cause order” rather than a warrant, it would have done so, as it did in the Wiretap Act.

Instead, as the Magistrate Judge recognized, Congress made clear that SCA warrants — like ordinary search and seizure warrants — are territorially limited and do not operate like *in personam* forms of process. *See* Decision at 17 (“The Government’s *in personam* jurisdiction argument is difficult to reconcile with the territorial limitations in Rule 41(b)” of the Federal Rules of Criminal Procedure.). Congress used the term of art “warrant” to invoke the traditional territorial limitations long associated with that term. *See F.A.A. v. Cooper*, 132 S. Ct. 1441, 1449 (2012) (“[W]hen Congress employs a term of art, ‘it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken.’”) (quoting *Molzof v. United States*, 502 U.S. 301, 307 (1992)). As the Eighth Circuit has noted in interpreting Section 2703, “Congress called them warrants and we find that Congress intended them to be

² Congress also demonstrated in the SCA that it could create specialized types of orders requiring providers to disclose information about their customers. *See* 18 U.S.C. § 2703(d) (describing requirements for a court order to obtain, e.g., subscriber record information, and requiring government to “offer[] specific and articulable facts showing that there are reasonable grounds to believe” that the records sought “are relevant and material to an ongoing criminal investigation”). If Congress intended to create, in Section 2703(a), a “probable cause order” for the disclosure of communications content, it would have done so.

treated as warrants.” *United States v. Bach*, 310 F.3d 1063, 1066, n. 1 (8th Cir. 2002); *see also In re 381 Warrants Directed to Facebook, Inc.*, ___ N.E.3d ___, 2017 WL 1216079, 2017 N.Y. Slip Op. 02586, at *5 (N.Y. Apr. 4, 2017) (“[T]he SCA plainly distinguishes between subpoenas and warrants, and there is no indication that Congress intended for SCA warrants to be treated as subpoenas. Indeed, to so hold would be to ignore the plain language of the SCA in contravention of the rules of statutory interpretation.”). Established rules of statutory interpretation require no less. *Conn. Nat’l Bank v. Germain*, 503 U.S. 249, 253-54 (1992) (“[C]ourts must presume that a legislature says in a statute what it means and means in a statute what it says there.”).

When Congress enacted the SCA, it understood that the private content of stored communications was protected by the Fourth Amendment, and that accessing them would entail a search and seizure. *See* H.R. Rep. No. 99-647, at 68 (1986) (“The Committee required the government to obtain a search warrant because it concluded that the contents of a message in storage were protected by the Fourth Amendment.”). Among the traditional characteristics of warrants are their territorial limitations; they are only effective to reach places and things found in the United States. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990) (holding that a warrant “would be a dead letter outside the United States”); *Second Circuit Decision*, 829 F.3d at 212 (“a warrant protects privacy in a

distinctly territorial way”). Congress also would have understood that “[s]earch warrants are not directed at persons; they authorize the search of ‘place[s]’ and the seizure of ‘things.’” *Zurcher v. Stanford Daily*, 436 U.S. 547, 555 (1978) (2nd alteration in original) (citation omitted).³ It is beyond question, for example, that an SCA warrant could not authorize the FBI to travel to a Google data center in, say, Singapore, demand access to the servers located there, and download from them communications otherwise within the scope of the warrant. And the FBI could not broaden the scope of its power under a warrant by compelling a third-party (like Google) to carry out a search that the FBI itself lacks the authority to carry out.

The Magistrate Judge thus correctly found that the SCA’s use of the term of art “warrant” and its legislative history do not reflect an intent by Congress to

³ While Federal Rule of Criminal Procedure 41 was modified on December 1, 2016, to permit magistrate judges to issue warrants to search out-of-district electronic information in certain circumstances not relevant here, nothing in the amended Rule contemplates a search of property that is or may be located outside the country. As the Department of Justice acknowledged in a letter to Advisory Committee on the Criminal Rules, “[i]n light of the presumption against international extraterritorial application, and consistent with the existing language of Rule 41(b)(3), this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries.” Letter from Mythili Raman, Acting Assistant Attorney Gen., to Judge Reena Raggi, Chair, Advisory Comm. on the Criminal Rules, at p. 4 (Sept. 18, 2013) (available at <https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf> (last accessed July 21, 2017)). Accordingly, the government cannot obtain a search warrant to search property outside the United States.

authorize searches or seizures of communications stored in locations in the United States. *See* Decision at 16-17. However, the Magistrate Judge erred in applying the second step of the *Morrison* test, as explained below.

B. Requiring a provider to execute a warrant to search and seize data outside the United States is an impermissible extraterritorial application of the SCA.

Under *Morrison*'s second step, when a statutory provision such as the Section 2703 warrant provision has no extraterritorial reach, conduct relevant to the statute's focus cannot occur abroad without violating the presumption against extraterritoriality; if relevant conduct does occur abroad, it will constitute "an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory." *RJR Nabisco*, 136 S. Ct. at 2101

Here, the Magistrate Judge erred in reasoning that, as long as a Fourth Amendment search or seizure does not occur abroad, no conduct relevant to the focus of the statute will occur outside of the United States. *See* Decision at 20 ("the Court concludes that the warrant calls for a search and not a seizure, and that the conduct relevant to the extraterritorial analysis — *i.e.*, the location of the search — occurs entirely in the United States."). In so reasoning, the Magistrate Judge misapplied *Morrison*, which asks courts to determine whether conduct *relevant to the statute's focus* occurs abroad; not to determine whether conduct that occurs abroad meets the technical definitions of constitutional concepts like "search" or

“seizure.”

The SCA’s focus is on protecting the privacy of electronic communications by carefully delineating the means by which law enforcement can obtain access to those communications. The SCA sets out different standards and procedures for compelling disclosure of different types of data so as to afford a level of protection commensurate with the user’s privacy interest in that data. But regardless of whether the statute’s focus is characterized as “privacy” or “compelled disclosure,” the steps a provider takes to assist in the execution of a warrant by querying its network to identify responsive communications located in data centers outside the United States, accessing those foreign-stored communications, and retrieving them to the United States for disclosure to the government, constitute conduct that is not only relevant to the focus of the SCA, but essential to its effectiveness. Requiring Google pursuant to the warrant to identify, access, and retrieve communications located on servers outside the United States would thus constitute an impermissible extraterritorial application of the SCA.

1. The SCA’s focus is protection of the privacy of electronic communications by regulating the particular means of compelling disclosure.

Congress enacted the SCA to ensure that the privacy of electronic communications is appropriately protected, including when the government seeks to compel a provider to access and disclose those communications. Senator Leahy,

one of the SCA's authors, described its purpose as "updat[ing] our legal privacy protections [to] bring[] them in line with modern telecommunications and computer technology." 132 Cong. Rec. S7991 (daily ed. June 19, 1986) (statement of Sen. Leahy). As the Department of Justice observed in guidance issued prior to this litigation, the SCA "sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers." See U.S. Dep't of Justice, Executive Office of the United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, at 115 (Aug. 2009), <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf> (last visited June 30, 2017) (hereinafter "DOJ Manual"); see also S. Rep. No. 99-541 at 5 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 ("[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment."), reprinted in 1986 U.S.C.C.A.N. 3555, 3559.

To achieve this purpose, Section 2701 protects the privacy of electronic communications by criminalizing unauthorized access to such communications that have been stored with a service provider. See 18 U.S.C. § 2701. Section 2702 protects the privacy of electronic communications by prohibiting service providers from voluntarily disclosing such communications, except under expressly enumerated circumstances. See *id.* § 2702. And Section 2703 protects the privacy

of electronic communications and other data by requiring the government to obtain a subpoena, an order, or a warrant before compelling a provider to disclose subscriber information, records regarding the use of a communications service, or the contents of communications, respectively. *See id.* § 2703. “The privacy protections contained in 18 U.S.C. §§ 2702 and 2703 provide the heart of the SCA.” Orin Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending it*, 72 Geo. Wash. L. Rev. 1208, 1218 (2004). These protections are, in the words of the *Morrison* Court, “the object[] of the statute’s solicitude.” *Morrison*, 561 U.S. at 267 (identifying certain transactions as the object of the Exchange Act’s solicitude); *see also Second Circuit Decision*, 829 F.3d at 217 (privacy is the focus of the SCA).⁴

2. Assisting in the execution of an SCA warrant is conduct that is necessary to the operation of the statute and therefore relevant to its focus.

Section 2703, under which the warrants were issued, protects the privacy of the content of electronic communications — the most sensitive data that law enforcement might seek — by imposing a correspondingly rigorous process, and requiring that the government obtain a warrant issued upon a showing of probable

⁴ The Court should not narrowly confine its inquiry regarding the focus of the statute to a single, isolated subsection, but rather take into account the whole statute and related legislation. *See Morrison*, 561 U.S. at 267 (taking into account the prologue of the Exchange Act in determining its focus); *Id.* at 268 (taking into account the related Securities Act of 1933).

cause before compelling a provider to assist the government in its search and seizure of electronic communications.⁵ When a provider, pursuant to a warrant, identifies responsive communications, accesses them, and hands them over to the government, these actions affect users' privacy. What is more, these steps are essential to the execution of Section 2703 warrant. Thus, when a provider is compelled to identify, access, and retrieve communications that are stored solely on foreign servers, conduct relevant to the focus of the statute necessarily occurs outside of the United States.

Congress chose to protect the privacy of basic subscriber information, records regarding the use of an electronic communications service using distinct forms of legal process. *See* 18 U.S.C. § 2703. For the first category, which Congress deemed least private, it chose a subpoena; for the second, it chose a court order. For the content of communications, which Congress deemed most private, Congress chose "the full protection of a warrant." *See* Orin Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 384 (2014). Unlike the subscriber information obtained with a subpoena or the customer records obtained with a court order, the communications obtained with a warrant

⁵ Although section 2703(b) provides that the government may use lesser legal process for certain types of communications under certain conditions, that subsection of the SCA has been found to be unconstitutional. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

are not the provider's business records or information conveyed to the provider by the customer; they are the customer's private communications, and obtaining them entails a search and a seizure in a sense not implicated by the other two categories of data. Given that the government could not use a warrant to itself do what it seeks to compel Google to do here — namely to access foreign servers, and identify and retrieve foreign-stored communications⁶ — it makes little sense to maintain that Google's conduct abroad is somehow irrelevant to the focus of the statute.

In order to produce to the government data stored outside the United States, Google must write a query to search databases located in countries outside of the United States; execute the query to search for files and file components stored in said databases; isolate the files and file components; reassemble the file components into files; and then retrieve those communications to the United States for production to the government. When an SCA warrant requires a provider to

⁶ The Supreme Court has recognized that when conducting a search and seizure of private communications, location matters. In *Riley v. California*, 134 S. Ct. 2473 (2014), the Court addressed whether law enforcement could search the mobile phone of a suspect incident to that suspect's arrest. The Court distinguished between searching communications stored locally on the suspect's phone and searching the suspect's "data located elsewhere . . . on remote servers," noting that the latter "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." *Id.* at 2491. Like the search the Court cautioned against in *Riley*, the search the government proposes in this case of a location outside the United States raises significant and distinct policy and privacy issues that Congress has not considered or addressed.

undertake this process to assist in the execution of the warrant, the steps necessary to the process constitute “conduct relevant to the focus” of the SCA.

Here, the Magistrate Judge correctly determined that warrants are territorially limited. *See* Decision at 17. However, the Magistrate Judge misapplied the second step of the *Morrison* test by ignoring relevant conduct and instead erroneously looking to principles of constitutional law to identify the location of the Fourth Amendment “search,” which he determined occurred within the United States, rather than abroad. *See id.* at 20-25. Whether a Fourth Amendment search or seizure occurs only after a provider retrieves and discloses foreign-stored communications is beside the point; the Magistrate Judge’s analysis ignores all of the other relevant (and essential) conduct that Google must undertake to disclose foreign-stored data in response to a warrant. Indeed, courts are not required to determine (as the Magistrate Judge did) a singular location for the “focus”; they are instead required to consider where all of the “conduct relevant to the focus of the statute” occurs. *See RJR Nabisco*, 136 S. Ct. at 2101 (“[I]f the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory.”); *see also Morrison*, 561 U.S. at 266 (“[I]t is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States. But the presumption against extraterritorial application would

be a craven watchdog indeed if it retreated to its kennel whenever *some* domestic activity is involved in the case.” (emphasis in original)).⁷

The fact that Google is located in the United States does not alter the basic fact that essential conduct occurs outside the United States. That Google has technology that permits it to easily control data located in faraway places does not mean that nothing happens in those faraway places. Indeed, the warrant purports to compel Google to do something the government cannot do itself: intentionally write and execute a command to search a foreign server. *See* DOJ Manual, at 58 (“In the event that United States law enforcement inadvertently accesses a computer located in another country, CCIPS, OIA, or another appropriate authority should be consulted immediately, as issues such as sovereignty and comity may be implicated.”). As the government has likewise recognized elsewhere, even though a “search may seem domestic,” where the search involves “data [that] is stored remotely outside of the United States,” “other countries may view matters

⁷ The Magistrate Judge is incorrect as a matter of law that “the conduct relevant to the extraterritorial analysis . . . occurs entirely in the United States.” Decision at 20. When the government or its agent copies the contents of e-mails, it constitutes a search and seizure for purposes of the Fourth Amendment. *United States v. Jefferson*, 571 F. Supp. 2d 696, 703-704 (E.D. Va. 2008) (“individuals possess a constitutionally protected right to preserve the privacy of information recorded in books and documents against government attempts to photograph, transcribe, or otherwise copy the information”); *see also* Orin Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 703 (2010) (when a copy of an e-mail is made “the person loses exclusive rights to the data” in that e-mail). Here, that copying necessarily occurs outside the United States.

differently,” and the government “may be required to take actions ranging from informal notice to a formal request for assistance to the country concerned.” DOJ Manual at 85.⁸ Given that communications subject to the warrant are stored abroad and cannot be retrieved to the United States and disclosed to the government without conduct that occurs outside the United States, the warrant necessarily “involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory.” *RJR Nabisco*, 136 S. Ct. at 2101.

C. The Court should decline to weigh policy interests Congress has not yet considered.

This case, and others like it, raise important policy issues regarding how best to protect the privacy of electronic communications and law enforcement’s ability

⁸ Indeed, some governments have enacted so-called “Blocking Statutes” to combat the ability of foreign governments to regulate persons and data within their country. See, e.g., Council Regulation (EC) No 2271/96 of 22 November 1996 (E.U. Blocking Statute); Law no. 80-538 of 16 July 1980 (French Blocking Statute); Federal Data Protection Act of 14 August 2009 (Federal Law Gazette I p. 2814) (German Blocking Statute). Moreover, the Irish Government and a German Member of the European Parliament filed amicus briefs in the Second Circuit Decision, arguing that the U.S. must respect foreign sovereignty and a country’s control over its citizens’ data stored within its territorial limits. See Brief of Amicus Curiae Ireland, In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985-CV, 2014 WL 733621, at 3 (2d Cir. Dec. 15, 2014); Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament, In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft, Corp., No. 14-2985-CV, 2014 WL 7277561, at *8 (2d. Cir. Dec. 19, 2014) (“The successful execution of the warrant at issue in this case... would thus undermine the protections of the EU data protection regime, even for data belonging to an EU citizen and stored in an EU country.”).

to investigate crimes when evidence may reside within a borderless, distributed, global communications network. Adjusting the SCA to this changed landscape will require resolution of numerous policy issues. For example, Congress might choose to extend the SCA's warrant power only to U.S. citizens' data wherever stored to encourage other nations to limit their laws applied to their providers similarly, and thus protect U.S. citizens' data wherever it may be stored against disclosure to foreign law enforcement. Congress might choose to extend the SCA's warrant power to data wherever located, but require law enforcement to provide notice to the government of the customer's country of nationality or residence before serving such a warrant on the provider. Or Congress might choose to allow execution of SCA warrants overseas when ordered by a federal court, but not by state or local courts.⁹ Because Congress did not consider these

⁹ Congress might also craft legislation that takes into account the potential that allowing the U.S. government to search communications stored outside the United States "will significantly deter the use of remote data management technologies by business and individuals, particularly their use of U.S. cloud services providers, and thereby undermine a significant contributor to U.S. economic growth." Brief of BSA: the Software Alliance et al. as Amici Curiae Supporting Appellant, *Microsoft Corp. v. United States*, No. 14-2985, 2014 WL 7213177, at *3 (2d Cir. Dec. 15, 2014). Indeed, both Congress and the government have acknowledged the need for legislation to address some of these complex and conflicting policy issues. This is a fact well appreciated by the Members of Congress who have introduced a bill proposing related amendments. *See* International Communications Privacy Act, S. 2986, H.R. 5323, 114th Cong. (2016); Letter from Peter J. Kadzik, Assistant Attorney General, Dep't of Justice Office of Legislative Affairs, to Hon. Joseph A. Biden, President of the Senate, at p. 1 (July 15, 2016),

issues when it enacted the SCA, the statute does not address them. *See* Kerr, *Next Generation*, 162 U. Pa. L. Rev., at 410 (“ECPA simply was not written with the territoriality problem in mind.”). It therefore would not be proper for the courts to wade into these issues.

The Supreme Court has admonished lower courts not to engage in such “judicial-speculation-made-law—divining what Congress would have wanted if it had thought of the situation before the court.” *Morrison*, 561 U.S. at 261. The proper role of the judiciary is instead “to give the statute the effect its language suggests, however modest that may be; not to extend it to admirable purposes it might be used to achieve.” *Id.* at 270. As with the statute at issue in *RJR Nabisco*, the proper question regarding the SCA in this case is “not whether we think ‘Congress would have wanted’ a statute to apply to foreign conduct ‘if it had thought of the situation before the court,’ but whether Congress has affirmatively and unmistakably instructed that the statute will do so.” *RJR Nabisco*, 136 S. Ct. at 2100 (citations omitted); *see also Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957) (Congress “alone has the facilities necessary to make fairly [the] important policy decision” whether a statute applies extraterritorially).

https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf (last visited July 21, 2017) (proposing to Congress legislation to address “potential conflicting legal obligations that U.S. electronic communications service providers . . . may face when required to disclose electronic data by foreign governments investigating serious crime, including terrorism”).

Congress has not so instructed in this case.

Although the SCA requires modernization and reform, it is for Congress in its legislative capacity, not the courts, confined as they are to the particular case or controversy before them, to give audience to public debate, weigh the competing policy interests, and enact a law that takes them into account.

IV. CONCLUSION

For the foregoing reasons, the Court should decline the recommendation of the Magistrate Judge, interpret the SCA as its text and established canons of interpretation require, and void or modify the warrant to the extent that it requires Google to access, retrieve, and disclose to the government customer communications stored in data centers located outside the United States.

DATED: July 24, 2017

PERKINS COIE LLP

By: /s/ Jeffrey D. Vanacore

Jeffrey D. Vanacore

JVanacore@perkinscoie.com

Todd M. Hinnen (admitted *pro hac vice*)

THinnen@perkinscoie.com

30 Rockefeller Plaza, 22nd Floor

New York, NY 10112-0085

Telephone: 212.262.6900

Attorneys for Nonparty Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 24th day of July, 2017, I filed the foregoing with the Clerk of Court by hand and by email to Judge Hammer's chambers (as instructed) and have served the following by email:

L. Judson Welle
Assistant U.S. Attorney
Cyber Crime Coordinator
U.S. Attorney's Office for the District of New Jersey
970 Broad Street, Newark, NJ 07102
jud.welle@usdoj.gov

Counsel for the United States

By: /s/ Jeffrey D. Vanacore
Jeffrey D. Vanacore
PERKINS COIE LLP
30 Rockefeller Plaza, 22nd Floor
New York, NY 10112-0085
Telephone: 212.262.6900

Attorneys for Nonparty Google Inc.

Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

IN RE SEARCH WARRANT MAG. NO.) Hon. Michael A. Hammer
16-4116 (MAH) TO GOOGLE INC.)
) Mag. No. 16-4116

STIPULATION

The government by its counsel, Paul J. Fishman, United States Attorney for the District of New Jersey, L. Judson Welle and Bruce P. Keller, Assistant U.S. Attorneys, and Andrew S. Pak, Trial Attorney, United States Department of Justice, Criminal Division, and Google Inc., by its counsel, Todd M. Hinnen, and Jeffrey D. Vanacore, Perkins Coie, LLP, hereby stipulate to the following facts, which may be found by the Court as true for the purposes of this matter:

1. Google Inc. ("Google") is a U.S.-headquartered company incorporated in Delaware with a principal place of business in California. Among other things, Google offers users a variety of different online and communications services.

2. Google stores user data in various locations, some of which are inside the United States and some of which are in countries outside the United States.

3. Some user files may also be broken into component parts, and different parts of a single file may be stored in different locations (and, accordingly, different countries) at the same time.

4. Google operates a state-of-the-art intelligent network that, with respect to some types of data including some of the data at issue in this case, automatically moves data from one location on Google's network to another as frequently as needed to optimize for performance, reliability and other efficiencies. As a result, the country or countries in which specific user data, or components of that data, is located may change. It is possible, therefore, that the network will change the location of data between the time when the legal process is sought and when it is served. In addition, for certain types of data, including some of the data at issue in this case, Google's tool that queries the network does not report the country in which foreign-stored data is located.

5. Only Google personnel in Google's Legal Investigations Support team are authorized to access the content of communications in order to produce it in response to legal process. All such Google personnel are located in the United States.

6. On December 19, 2016, Google's Legal Investigations Support team received from the government a search warrant ("the Warrant") seeking certain records associated with three Google email accounts (the "Target Accounts 1, 2, and 3").

7. Google undertook diligent efforts to identify responsive information that was located in the United States. For the Target Accounts, Google retrieved from its network all records called for by the Warrant that Google

could confirm to be stored in the United States, and produced them to the government on January 6, 2017.


8. On April 25, after developing improved tools, Google made a supplemental production to the government of all remaining records stored in the United States.

9. In sum, Google has produced responsive records as follows:

- a. For Target Accounts 1 and 3, Google has produced: (a) current and preserved subscriber information; (b) device information; (c) preserved Gmail content; (d) Gmail content; and (e) correspondence between Google and the accountholders. For Target Account 1, Google did not produce attachments to emails only to the extent those files were stored on servers located outside the United States.
- b. For Target Account 3, Google has produced all records called for by the Warrant .
- c. For Target Account 2, Google has produced: (a) preserved subscriber information, and (b) current subscriber information, which are all the records called for by the Warrant that are available to Google. Google has no further records to produce for Target Account 2 because the user deleted the account before Google received the Warrant (or the preceding preservation letter).

10. As of April 25, 2017, Google had produced all responsive records stored in the United States.

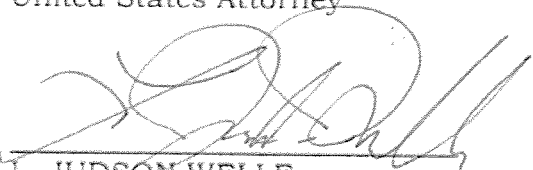
For GOOGLE INC.



TODD M. HINNEN
JEFFREY D. VANACORE
Attorneys for Google Inc.
PERKINS COIE, LLP

For THE UNITED STATES

PAUL J. FISHMAN
United States Attorney



L. JUDSON WELLE
BRUCE P. KELLER
Assistant U.S. Attorneys

ANDREW S. PAK
Trial Attorney
U.S. Department of Justice